Introduction to Security

Ms. Tommie Abrams
Security Branch

PERS-534C
Wood Hall, Bldg 769, Room 184

Your Security Team

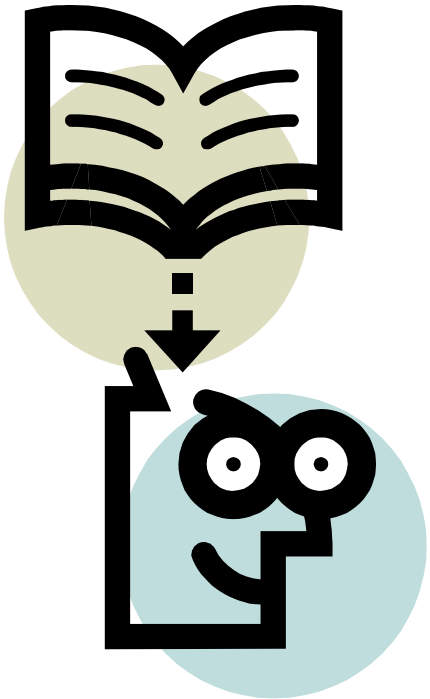
Daniel Harris	Command Security Manager	4-3091
Trisha Dooley	EKMS / COMSEC	4-5353
Tommie Abrams	Security Awareness Training Officer Antiterrorism Training Officer Mail Manager	4-3089
David McGhee	Mail Clerk	4-3138
Carla Karpen	Personnel Security Top-Secret Control Officer NATO Control Officer	4-3082
Daniel Boucher	Personnel Security Specialist	4-3084
Theresa Law	Personnel Security Technician	4-3088

References

- **DODD 5205.02 - DOD Operations Security (OPSEC) Program**
- **DOD 5220.22M – National Industrial Security Program**
- **SECNAVINST 5239.3A - DON Information Assurance (IA) Policy**
- **SECNAV M-5510.30 - DON Personnel Security Program**
- **SECNAV M- 5510.36 - DON Information Security Program**
- **OPNAVINST 5239.1 - DON Information Assurance Manual**
- **OPNAVINST 5530.14E - Navy Physical Security & Law Enforcement**
- **BUPERSINST 5239.1B - BUPERS Information Systems Security (INFOSEC) Program**
- **NAVPERSCOMINST 5510.1 - NPC Security Program**
- **NAVPERSCOMINST 5530.1 - NPC Physical Security, Loss Prevention & Anti-Terrorism**

Major Elements

- Personnel Security
- Information Security
- Computer Security
- Physical Security
- Industrial Security
- Operations Security



Personnel Security

Personnel Security

Civilians, military and contractors must

possess a valid security investigation

consistent with the interests of National

Security per SECNAV M-5510.30

Personnel Security (Con't)

Adjudication Guidelines SECNAV M-5510.30, Appendix G

- Allegiance to the United States
- Foreign influence
- Foreign preference
- Sexual behavior
- Personal conduct
- Financial considerations
- Alcohol consumption
- Drug involvement
- Emotional, mental, and personality disorders
- Criminal conduct
- Security violations
- Outside activities
- Misuse of Information Technology

Information Security

YOU are the key component of all of our security efforts

Access to Classified Information

- Appropriate Investigation
  - Adjudicated for specific level of Classified information (Top Secret, Secret, Confidential)
- Approved Access
  - Authorized by PERS-534
- Need to Know
  - Job Requirement

Handling Procedures

- Store classified diskettes and removable media in appropriate approved security safes when not in use
- Dispose/destroy printed materials and data as prescribed in SECNAV M-5510.36
- Do not discuss classified information in an Unclassified/Unsecured environment (Telephone)
- Never remove classified information from command without authorization from Command Security Manager
- Only use SIPRNET or Secure Fax to transmit classified information

Compromise

- Loss of classified information that cannot be physically located or accounted for
- Classified information placed and routed in guard mail envelopes or on unclassified LAN
- Classified information not properly controlled and stored
- Unauthorized disclosure
- Electronic Spillage (classified information placed on an unclassified computer system)

Report any loss or compromise of classified information to Command Security Manager at 4-3091 immediately

Mailing

- SECNAV M-5510.36 provides the procedures for mailing classified information
- Any questions call PERS-534

Computer Security

YOU are the key component of all of our security efforts

Computer Security - General Info

- BUPERSINST 5239.1B
- Use of personal computer software or hardware is not authorized on any Navy system
- NO desk top modems authorized
- Use of computer games is prohibited
- Report security incident to appropriate Information Assurance Officer (IAO)– virus or classified spillage
- Use your government computer for Official Business Only

Physical Security

YOU are the key component of all of our security efforts

Physical Security

- Naval Support Activity Mid-South (NSA) is responsible for overall security of the base including:
  - Protection of property
  - Protection of personnel
  - Temporary or permanent debarment

Physical Security - Safes

- Ensure only authorized individuals have access to safes containing classified information
- Use SF-701, Activity Security Checklist, for spaces storing classified information
- Use SF-702, Security Container Check Sheet, when opening and closing safe
- Ensure SF-700, Security Container Information form, is completed and taped inside safe to display authorized personnel with access to safe
- Ensure OF-89, Maintenance Record, is taped on the inside of safe

Physical Security – Emergency Exits

- Do not go out emergency exits unless it is an Emergency

Mission Essential – Selection Criteria

Personnel or function is identified as essential by their Department, Staff Office Directorate (SOD), or Special Assistant (SA), vital to the operational readiness or mission effectiveness of the command's mission.

Personnel assigned as essential must be available on demand or on call.

Force Protection Conditions (FPCONS)

Normal	No Known Threat
Alpha	General Threat That Possible Terrorist Activity Exists
Bravo	There is an Increase/More Predictable Threat of Terrorist Activity Exists
Charlie	An Incident Has Occurred or Intelligence Received Indicating Terrorist Action Imminent
Delta	Attack Has Occurred or When Intel Received That a Terrorist Action Against a Specific Location or Person is Imminent.

Force Protection Conditions (FPCONS)

Normal Alpha Bravo	Normal routine and Random Anti-Terrorism Measures (RAM) exercises being conducted. Added security by NSA at gates
Charlie	Requirements of Normal, Alpha and Bravo. NPC will go to a single entrance/exit for access to NPC buildings, and set a Security/Roving Patrol Watch in each building. Watch will search all parcels and ensure all personnel entering the buildings have swiped their CAC card and entered PIN number for access (no piggy backing)

Force Protection Conditions (FPCONS)

Delta	All measures from previous FPCONs will be applied. Only essential personnel will report to work. Building Security/Roving Patrol Watch will continue in all buildings with personnel present. All personnel entering NPC buildings will sign in and out. Only those personnel with proper drive-on badges are permitted drive-on base access, all other personnel will park in the area assigned at Mid-South Conference Center for walk-in/shuttle base access.

Force Protection Conditions (FPCONS)

Delta	When FPCON DELTA is set, all NPC Personnel will be notified or informed via local TV and radio of NSA Mid-South - Open For Essential Personnel Only. NPC personnel are encouraged to call 874-7474 for further information about base closure and openings. For complete information on NPC FPCON measures please refer to NAVPERSCOMINST 5530.1, Physical Security, Loss Prevention, and Anti-terrorism

Industrial Security - Contractors

- Reference – DoD 5220-22M

Operations Security (OPSEC)

YOU are the key component of all of our security efforts

Definition

- OPSEC is a risk management tool used to deny an adversary information generally unclassified but critical/sensitive concerning our intentions and capabilities

- What is critical/sensitive information?
  - Information about our activities, intentions and capabilities, that an adversary needs to gain an advantage

Examples

- Troop Deployment
- Weapon Systems Technology
- Local Exercises
- Test Schedules

Adversaries

- International Terrorists Groups
- Foreign Intelligence Agencies
- Hackers
- Other Types of Adversaries
  - Disgruntled Employees
  - Dishonest Employees

Communication

- Internet
- Cellular Phones
- Fax Machines
- Unsecured Communication Lines

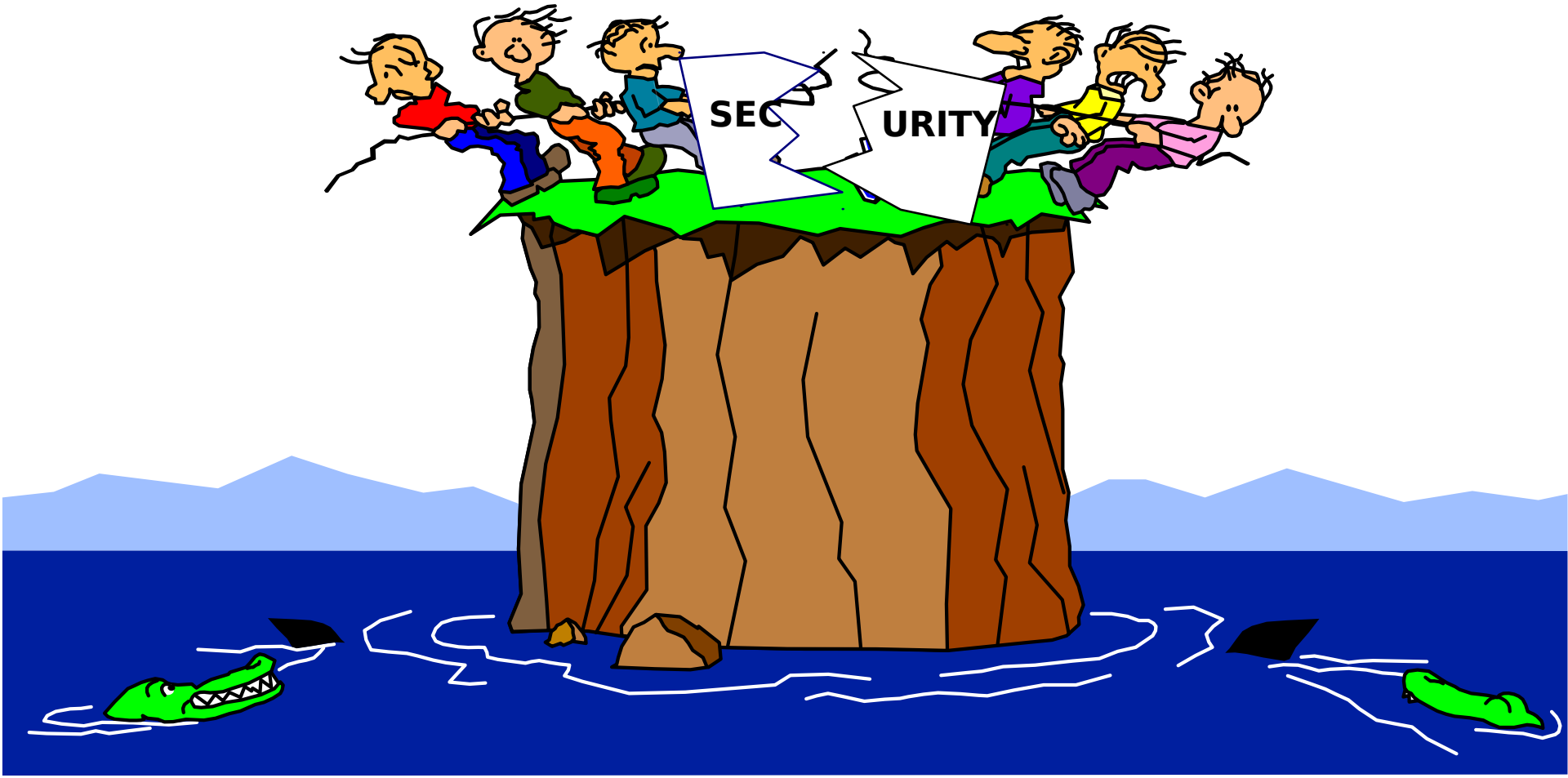
Rules to Live By

- Don’t discuss readiness Issues
- Don’t discuss specific training exercises
- Don’t assume the enemy is not trying to collect information

Key Points

- Good OPSEC save lives and resources
- Always use common sense and be aware
- Review procedures for destruction of sensitive information

Teamwork is Essential



YOU are the key component of all of our security efforts

Visit our website NPC Security Website

Video Time

–

My Time is Up…Thank You